onelogin

Data Trust and Security at OneLogin

3rd March 2020.

Table of Contents

Trust & Security Today at OneLogin

"Security First" is today how we operate at OneLogin.

Our Global Enterprise Trust and Security program is led by Vanessa Pegueros, Chief Trust & Security Officer (CTSO), who reports directly to OneLogin's Chief Executive Officer (CEO), Brad Brooks.

The program scope covers our technologies, business processes and security culture across the global operating environments of our production and our corporate facilities.

Our Trust and Security function has dedicated teams carrying out focused risk assessments throughout our technology and data management lifecycle. The scope of these risk assessments include our service partners, suppliers, and vendors. Our Security Engineers design the security controls in our product and corporate service offerings. Our Application Security team has an independent mandate to test our technologies, to provide Trust Assurance that threat vectors and their associated vulnerabilities have appropriate controls applied to reduce the number of confidentiality, integrity, availability and privacy risks to an acceptable business operating level.

With the ever changing threat landscape, we have put in place a dedicated monitoring, incident response and investigation team. The team has a global operations remit to continue to build a best in class incident response. A fundamental component to this is working with our Customers and Partners via our dedicated 'Responsible Disclosure' program.

This program alerts us to vulnerabilities that we need to investigate and address to continue to protect our OneLogin environment and collaborate with you, our Customers and Partners, to protect the global ecosystem from malicious attackers. Please see Security section of our website for more details on Security and our Responsible Disclosure program: https://www.onelogin.com/security

All reported threats and their associated vulnerabilities are now investigated by OneLogin's Incident Response and Investigations team. The investigation process categorizes each threat, and assigns it a risk category rating based on the technology service, the data it processes, any associated information assets and most importantly an assessment of the vulnerability factors. From this, the incident is prioritised and remediation actions are implemented.

OneLogin is equipped for a defense in-depth incident response. This starts with our "Security First" culture and dedication to security by design principle. Our dedicated Security program management function provides trust assurance in relation to security controls and their implementation and associated operational management. Therefore, creating an incident response reduces business impacts for not only OneLogin but our Customers and Partners avoiding all the consequences of a data breach.

Data is at the Core of our Trust & Security Framework

Data Management is at the core of the OneLogin Trust and Security framework. The framework is built from a full range of factors that inform the security approach, from the broadest government laws and regulations to the details of specific contractual agreements. OneLogin then takes all these externally focused factors to translate them into our internal policies, standards and procedures that make up how we at OneLogin operate. This includes how we provide you with Trust Assurance for the management of Customer Data. Below we detail the five layers of our Data Trust and Security Framework:

1. Global, Federal & State Laws

OneLogin works at international and global level to stay abreast of security and privacy requirements as set forth under international, federal and state laws. By continually monitoring the security and privacy landscape, OneLogin can modify its data governance approach to remain in step and comply with the latest requirements.

2. Government Regulatory Privacy and Security Requirements

OneLogin demonstrates it is committed to providing Trust Assurance to its customers by maintaining a robust control environment that meets and exceeds compliance with government regulations and frameworks around the world that were developed to ensure the privacy and security of personal and sensitive confidential information, including:

General Data Protection Regulation (GDPR) – The GDPR is a European Union (EU) data protection law that requires organizations that process personal data to be responsible for that data and stipulates requirements for handling personal data and documenting those practices. OneLogin is committed to data privacy. Its strong compliance culture, policies, and robust security safeguards reflected in its ISO 270018 certification provide a solid foundation for the company's continued GDPR efforts.

The California Consumer Privacy Act (**CCPA**) - This state statute is intended to enhance privacy rights and consumer protection for residents of California. OneLogin's Privacy Program is aligned to meet the privacy principle requirements.

3. Industry Compliance Regulations

OneLogin's security and privacy program operating models are further informed by regulations in specific industries. Our OneLogin product and service offerings enables organizations to demonstrate compliance with industry regulations and includes authentication, authorization assurances providing detailed information on who, when, where and how a system was accessed.

OneLogin continually reviews its security capabilities in light of new regulations as they are released.

4. Industry Best Practice Standards

Regardless of the industry, the need for data governance has driven the creation of best practices and standards to guide companies in their security and privacy strategy and capabilities. OneLogin provides its customers with Trust Assurance on how their data is protected and managed via our certifications and attestations to industry best practice standards. OneLogin Trust Assurance earned, includes:

ISO 27001:2013 – The highest level of certification available today for assuring global information security. OneLogin has earned this certification for all aspects of the enterprise, including the OneLogin Product and Service Offering along with our company operations. ISO 27001 is core to OneLogin's Security Standard model, and OneLogin's ISO 27001 results can be made available to customers so that they can map them into their own vendor management programs.

ISO 27017:2015 – This standard provides guidance to both cloud service providers and consumers of these services in the form of objectives, controls, and guidelines. OneLogin aligned its existing security controls to be compliant to this standard in order to augment its security program. These controls are tested as part of the periodic SOC 2 Type 2 report and an independent body has audited our compliance with this standard as part of our ISO 27001:2013 certificate annual audits.

SOC 1 Type 2, SOC 2 Type 2 – Provides confirmation of OneLogin's financial and information security controls. A SOC 1 Type 2 report describes the internal controls in place over financial reporting at an organizational level and requires a third-party service auditor to review and examine the organization's operations over a set period of time. The SOC 2 Type 2 report specifically indicates that OneLogin's technology meets the criteria for security, availability, confidentiality, and processing integrity and confirms that it is protected against unauthorized physical and logical access. The report also confirms the platform is available for operation and use as an information system designated as confidential and protected, and that it is complete, accurate, timely, and authorized.

PCI DSS – The Payment Card Industry Data Security Standard outlines the security requirements for organizations that process, manage and store cardholder data. As a data processor OneLogin is in alignment with supporting organizations that meet their PCI-DSS Compliance requirements.

Skyhigh CloudTrust – OneLogin aligns to the mandated stringent requirements for the protection, identity verification, and security controls of cloud-based data, based on detailed criteria developed in conjunction with the Cloud Security Alliance.

CSA STAR – OneLogin has been proactive in working with the Cloud Security Alliance whose mission is to promote best practice in the provision of security assurance within Cloud Computing.

5. Customer Contractual Agreements

OneLogin provides assurance to customers about data governance for privacy and security with the OneLogin Trust Experience Platform and associated product and service offerings, which are outlined in OneLogin's contractual agreements. Example clauses include, but are not limited to, our EU model contract clauses and/or our data security addendum. These contractual commitments will continue to provide Trust Assurance for our British customers with the implementation of Brexit.

Continuous Improvement Commitment

Protecting data against the ever changing threat landscape requires constant and continuous focus. At OneLogin our Trust and Security team work daily to deliver that. We work with independent industry leaders for support and provide assurance via security security assessments and testing.

Independent Penetration Testing - This testing is carried out on a quarterly basis. The objective of these tests is to help ensure we discover potential security vulnerabilities that may impact service and/or data processed through the service.

OneLogin Trust and Security Assurance

"Security First" is today how we operate at OneLogin.

We continue to provide our Customers, Partners, Suppliers and Prospects with Trust and Security Assurance via the program we operate. For further information please visit OneLogin Trust: https://www.onelogin.com/trust. Alternatively you can reach out to us via your Customer Account Management or directly at Security@OneLogin.com